

receiving objects over a computer network, each received object being associated with a user account to store the received object on the shared storage system;  
 storing the received objects on the computer storage of the shared storage system, each received object being stored in a manner indicating the user account that stored the received object in the shared storage system;  
 marking an object from among the objects stored on the shared storage system as containing prohibited content;  
 in response to the marking of an object as containing prohibited content, storing incident data in an incident history record in the computer storage, the incident data indicating at least the user account that stored the marked object in the shared storage system;  
 processing the incident history record for incident data associated with a selected user account;  
 modifying an access privilege of the selected user account according to rules applied to at least the incident data in the incident history record associated with the selected user account as processed from the incident history record;  
 in response to a request to access an object from among the stored objects,  
   determining if content in the requested object is marked as containing prohibited content; and  
   in response to a determination that the content in the requested object is marked as containing prohibited content, limiting access to the content from the requested object as stored in the shared storage system.

11. The article of manufacture of claim 10, wherein modifying comprises terminating privileges of the user account to share objects with other user accounts.

12. The article of manufacture of claim 10, wherein the object is a file and limiting access to content in the object includes preventing access to a file stream containing the prohibited content.

13. The article of manufacture of claim 10, wherein the process further comprises:  
   allowing the object that is marked as containing prohibited content from a first user account to be shared with one or more second user accounts;  
   limiting access through the one or more second user accounts to the prohibited content in the object.

14. The article of manufacture of claim 10, wherein the process further comprises:  
   displaying an indication that the object is marked as including prohibited content.

15. A computer storage system comprising:  
 shared computer storage in which objects are stored containing content, the objects being received over a computer network from user computers, each received object being stored in a manner indicating a user account that stored the received object in the shared storage system;

one or more processing devices, connected to the shared computer storage, programmed to:  
 mark an object from among the objects stored on the shared computer storage as containing prohibited content;  
 in response to marking an object as containing prohibited content, store incident data in an incident history record on the shared computer storage, the incident data indicating at least the user account that stored the marked object in the shared storage system;  
 process the incident history record for incident data associated with a selected user account;  
 modify an access privilege of the selected user account according to rules applied to at least the incident data in the incident history record associated with the selected user account as processed from the incident history record; and  
 in response to a request to access an object from among the objects stored on the shared computer storage, and in further response to a determination that the content included in the requested object is marked as prohibited, limit access to the content included in the requested object from the shared computer storage.

16. The computer storage system of claim 15, the one or more processors being programmed to:  
   allow a group of objects from a first user account to be shared with one or more second user accounts;  
   determining if the group of objects includes an object that is marked as containing prohibited content;  
   limiting access by the one or more second user accounts to the prohibited content in the object that is marked, while allowing access through the one or more second user accounts to other objects in the group of objects.

17. The computer storage system of claim 15, further comprising one or more server computers, including the one or more processors, and connected to a computer network, wherein a plurality of computers access the one or more server computers over the computer network to access objects stored on the storage.

18. The computer storage system of claim 15, the one or more processors being programmed to cause an indication to be displayed that an object being accessed includes prohibited content.

19. The computer storage system of claim 15, wherein to modify an access privilege, the one or more processors are further programmed to terminate privileges of the user account to share objects with other user accounts.

20. The computer storage system of claim 15, wherein the one or more processors are further programmed to:  
   allow sharing from a first user account, with one or more second user accounts, the object that is marked as containing prohibited content;  
   limit access through the one or more second user accounts to the prohibited content in the shared object.

\* \* \* \* \*